(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001077802 A**

(43) Date of publication of application: **23.03.01**

(51) Int. Cl **H04L 9/08**
G06F 12/14
G11B 20/10
H04N 5/84
H04N 5/91

(21) Application number: **11248420**

(22) Date of filing: **02.09.99**

(71) Applicant: **SONY CORP**

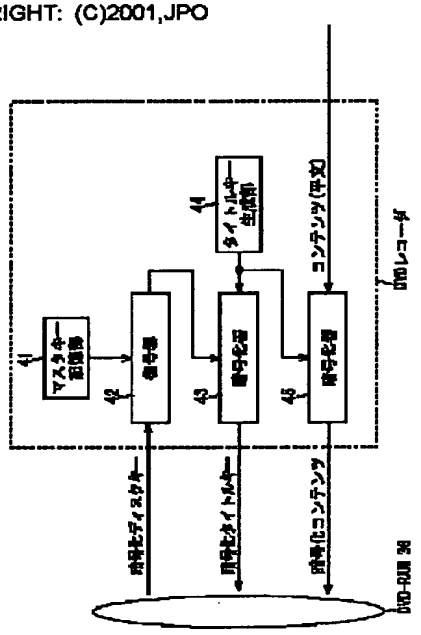
(72) Inventor: **OSAWA YOSHITOMO**
ASANO TOMOYUKI

(54) DATA PROVIDING DEVICE, DATA PROVIDING METHOD, PROGRAM RECORDING MEDIUM, DATA RECORDING MEDIUM AND MANUFACTURE OF DATA RECORDING MEDIUM

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent an illegal copy to a DVD-RAM and to reproduce the DVD-RAM to which the legal copy is made by using an existing DVD player.

SOLUTION: A disk key encrypted by a master key (encrypted disk key) is stored in advance in a DVD-RAM 36, a decoder 42 reads the encrypted disk key from the DVD-RAM 36 and decodes it by using the master key stored in a master key storage section 41. Furthermore, an encryption device 43 encrypts the title key outputted from a title key generating section 44 by using the master key decoded by the decoder 42 and stores the encrypted title key obtained as a result to the DVD-RAM 36. Then an encryption device 45 encrypts contents by using the title key outputted from the title key generating section 44 and stores it to the DVD-RAM 36.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－77802
（P2001－77802A）
(43)公開日　平成13年３月23日(2001.3.23)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｃ０５２
			３２０Ｅ	５Ｃ０５３
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｄ０４４
Ｈ０４Ｎ　5/84		Ｈ０４Ｎ　5/84	Ｚ	５Ｊ１０４

審査請求　未請求　請求項の数16　ＯＬ　（全 19 頁）　最終頁に続く

(21)出願番号　特願平11－248420

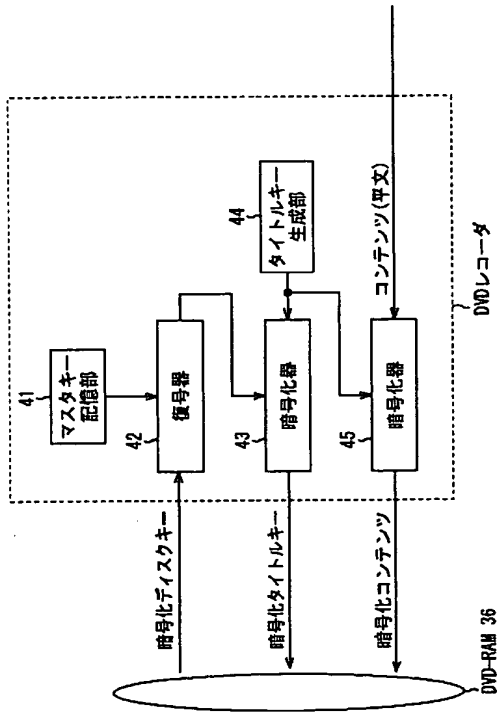
(22)出願日　平成11年９月２日(1999.9.2)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　大澤　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

最終頁に続く

(54)【発明の名称】　データ提供装置、データ提供方法、およびプログラム記録媒体、並びにデータ記録媒体、およびデータ記録媒体の製造方法

(57)【要約】
【課題】　ＤＶＤ－ＲＡＭに対する違法コピーを防止するとともに、適法なコピーが行われたＤＶＤ－ＲＡＭを、現行のＤＶＤプレーヤで再生する。
【解決手段】　ＤＶＤ－ＲＡＭ３６には、マスタキーで暗号化されたディスクキー（暗号化ディスクキー）があらかじめ記録されており、復号器４２は、暗号化ディスクキーを、ＤＶＤ－ＲＡＭ３６から読み出し、マスタキー記憶部４１に記憶されているマスタキーで復号する。さらに、暗号化器４３は、タイトルキー生成部４４が出力するタイトルキーを、復号器４２が復号したマスタキーで暗号化し、その結果得られる暗号化タイトルキーを、ＤＶＤ－ＲＡＭ３６に記録する。そして、暗号化器４５は、コンテンツを、タイトルキー生成部４４が出力するタイトルキーで暗号化し、ＤＶＤ－ＲＡＭ３６に記録する。



1

【特許請求の範囲】

【請求項１】　データを暗号化して提供するデータ提供装置であって、

第１キーで暗号化された第２キーである暗号化第２キーを取得する取得手段と、

前記暗号化第２キーを、前記第１キーに基づいて復号する暗号化第２キー復号手段と、

前記暗号化第２キー復号手段により復号された前記第２キーを利用して、前記データを暗号化する暗号化手段と、

前記暗号化手段により暗号化された前記データである暗号化データを提供する提供手段とを含むことを特徴とするデータ提供装置。

【請求項２】　前記暗号化手段は、

第３キーを、前記第２キーで暗号化し、暗号化第３キーを出力する第３キー暗号化手段と、

前記データを、前記第３キーで暗号化するデータ暗号化手段とを有し、

前記提供手段は、前記暗号化データを、前記暗号化第３キーとともに提供することを特徴とする請求項１に記載のデータ提供装置。

【請求項３】　前記第１キーを記憶している記憶手段をさらに含むことを特徴とする請求項１に記載のデータ提供装置。

【請求項４】　前記取得手段は、複数の第１キーそれぞれで暗号化された第２キーである暗号化第２キーのセットのうち、前記記憶手段に記憶されている前記第１キーで復号可能なものを取得することを特徴とする請求項３に記載のデータ提供装置。

【請求項５】　前記暗号化第２キー復号手段による復号方法、および前記暗号化手段による暗号化方法は、ＤＶＤ(Digital Versatile Disc)規格に準拠したものであることを特徴とする請求項１に記載のデータ提供装置。

【請求項６】　前記取得手段は、データ記録媒体に記録された前記暗号化第２キーを読み出すことを特徴とする請求項１に記載のデータ提供装置。

【請求項７】　前記取得手段は、伝送路を介して伝送されてくる前記暗号化第２キーを受信することを特徴とする請求項１に記載のデータ提供装置。

【請求項８】　前記提供手段は、前記暗号化データを、データ記録媒体に記録することを特徴とする請求項１に記載のデータ提供装置。

【請求項９】　前記提供手段は、前記暗号化データを、伝送路を介して伝送することを特徴とする請求項１に記載のデータ提供装置。

【請求項１０】　データを暗号化して提供するデータ提供方法であって、

第１キーで暗号化された第２キーである暗号化第２キーを取得する取得ステップと、

前記暗号化第２キーを、前記第１キーに基づいて復号する暗号化第２キー復号ステップと、

2

前記暗号化第２キー復号ステップにおいて復号された前記第２キーを利用して、前記データを暗号化する暗号化ステップと、

前記暗号化ステップにおいて暗号化された前記データである暗号化データを提供する提供ステップとを含むことを特徴とするデータ提供方法。

【請求項１１】　データを暗号化して提供するデータ提供処理を、コンピュータに行わせるためのプログラムが記録されているプログラム記録媒体であって、

第１キーで暗号化された第２キーである暗号化第２キーを取得する取得ステップと、

前記暗号化第２キーを、前記第１キーに基づいて復号する暗号化第２キー復号ステップと、

前記暗号化第２キー復号ステップにおいて復号された前記第２キーを利用して、前記データを暗号化する暗号化ステップと、

前記暗号化ステップにおいて暗号化された前記データである暗号化データを提供する提供ステップとを含むプログラムが記録されていることを特徴とするプログラム記録媒体。

【請求項１２】　データが暗号化されて記録される記録可能なデータ記録媒体であって、

第１キーで暗号化された第２キーである暗号化第２キーが記録されており、

後に、前記暗号化第２キーを、前記第１キーで復号し、前記第２キーを得て、その第２キーを利用して、前記データが暗号化されて記録されることを特徴とするデータ記録媒体。

【請求項１３】　ＤＶＤ(Digital Versatile Disc)規格に準拠したフォーマットを有することを特徴とする請求項１２に記載のデータ記録媒体。

【請求項１４】　複数の第１キーそれぞれで暗号化された第２キーである暗号化第２キーのセットが記録されていることを特徴とする請求項１２に記載のデータ記録媒体。

【請求項１５】　前記暗号化第２キーは、読み出しが可能であるが、書き込みが不可能な記録領域に記録されていることを特徴とする請求項１２に記載のデータ記録媒体。

【請求項１６】　データが暗号化されて記録される記録可能なデータ記録媒体の製造方法であって、

後に、第１キーで暗号化された第２キーである暗号化第２キーを、前記第１キーで復号し、前記第２キーを得て、その第２キーを利用して、前記データが暗号化されて記録されるデータ記録媒体に、前記暗号化第２キーを記録することを特徴とするデータ記録媒体の製造方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データ提供装置、

データ提供方法、およびプログラム記録媒体、並びにデータ記録媒体、およびデータ記録媒体の製造方法に関し、特に、例えば、ＤＶＤ－ＲＡＭ(Digital Versatile Disc - Random Access Memory)に対する違法コピーを防止するとともに、適法なコピーが行われたＤＶＤ－ＲＡＭを、現行のＤＶＤプレーヤで再生することができるようにするデータ提供装置、データ提供方法、およびプログラム記録媒体、並びにデータ記録媒体、およびデータ記録媒体の製造方法に関する。

【０００２】

【従来の技術】ディジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、ディジタル的に記録する記録装置や記録媒体が普及しつつある。

【０００３】このような記録装置および記録媒体によれば、例えば、画像や音声を劣化させることなく記録を繰り返すことができるため、即ち、画質や音質を維持したまま、何度もコピーすることができるため、そのようなコピーが違法に行われた記録媒体が、市場に流通すれば、映画等の著作権者等の利益が害されることになる。そこで、記録装置および記録媒体には、違法なコピーを行うことができないような仕組み（システム）が導入されている。

【０００４】即ち、例えば、ミニディスク装置においては（ミニディスクは商標）、違法なコピーを防止する方法として、ＳＣＭＳ(Serial Copy Management System)が採用されている。ＳＣＭＳは、再生側において、オーディオデータとともに、ＳＣＭＳ信号を、ディジタルインタフェース（ＤＩＦ）から出力し、記録側において、再生側からのＳＣＭＳ信号に基づいて、同じく再生側からのオーディオデータの記録を制御することにより、違法なコピーを防止するようになっている。

【０００５】即ち、ＳＣＭＳ信号は、オーディオデータが、コピーフリーのもの（copy free）であるか、１度だけコピーが許されているもの（copy once allowed）であるか、またはコピーが禁止されているもの（copy prohibited）であるかを表す信号で、記録側では、ＤＩＦからオーディオデータを受信すると、そのオーディオデータとともに送信されてくるＳＣＭＳ信号を検出する。そして、ＳＣＭＳ信号が、copy freeとなっている場合には、オーディオデータを、ＳＣＭＳ信号とともに、ミニディスクに記録する。また、ＳＣＭＳ信号が、copy once allowedとなっている場合には、ＳＣＭＳ信号を、copy prohibitedに変更して、オーディオデータとともに、ミニディスクに記録し、ＳＣＭＳ信号が、copy prohibitedとなっている場合には、オーディオデータの記録を行わない。

【０００６】以上のようにして、ミニディスク装置では、ＳＣＭＳによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

【０００７】しかしながら、ＳＣＭＳでは、上述のように、ＳＣＭＳ信号に基づいて、再生側からのオーディオデータの記録を制御するようにはなっていないミニディスク装置が製造された場合に対処するのが困難である。

【０００８】そこで、例えば、ＤＶＤプレーヤでは、コンテンツスクランブルシステムを採用することにより、著作権を有するデータが、違法にコピーされるのを防止するようになっている。

【０００９】コンテンツスクランブルシステムでは、ＤＶＤ－ＲＯＭ(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキーが、ライセンスを受けたＤＶＤプレーヤに与えられる。ライセンスは、ＤＶＤプレーヤを、不正コピーを行わない等の所定の動作規定にしたがうように設計することを条件に与えられ、従って、ライセンスを受けたＤＶＤプレーヤでは、与えられたキーを利用して、暗号化されたデータを復号することにより、ＤＶＤ－ＲＯＭに記録された画像や音声を再生することができる。一方、ライセンスを受けていないＤＶＤプレーヤは、暗号化されたデータを復号するためのキーを有していないため、その復号を行うことができず、これにより、ライセンス時に要求される条件を満たしていないＤＶＤプレーヤによって、ＤＶＤ－ＲＯＭが再生されることによる、不正なコピーが防止されるようになっている。

【００１０】コンテンツスクランブルシステムで採用されているＤＶＤ－ＲＯＭは、図１に示すように製造される。

【００１１】即ち、コンテンツ供給者である、映画会社その他の著作権者等は、ディスクキーとタイトルキーと呼ばれる、ＤＶＤ－ＲＯＭに記録される映画等のコンテンツの暗号化および復号に利用される２つのキーを決定して発行する。

【００１２】鍵管理センタ４は、ＤＶＤプレーヤの製造に用いられるＬＳＩ(Large Scale Integrated Curcuit)やソフトウェアモジュールのメーカに割り当てる複数のマスタキーを設定し、暗号化器５において、その複数のマスタキーそれぞれで、ディスクキーを暗号化することにより、暗号化されたディスクキー（以下、適宜、暗号化ディスクキーという）のセットを作成する。さらに、暗号化器６において、ディスクキーで、タイトルキーが暗号化され、暗号化されたタイトルキー（以下、適宜、暗号化タイトルキーという）が作成される。そして、鍵管理センタ４は、暗号化ディスクキーのセットと、暗号化タイトルキーを、ＤＶＤ－ＲＯＭの製造業者であるディスク製造業者７に提供する。

【００１３】ディスク製造業者７では、圧縮器２において、データベース１に登録されている画像や音声等のディジタルデータであるコンテンツが、例えば、ＭＰＥＧ(Moving Picture Experts Group)２方式によって圧縮さ

れ、暗号化器３において、圧縮器２が出力するコンテンツが、コンテンツ供給者が発行するタイトルキーで暗号化され、暗号化コンテンツとされる。

【００１４】さらに、ディスク製造業者７では、暗号化コンテンツとともに、鍵管理センタ４から提供される暗号化ディスクキーのセットと暗号化タイトルキーが記録されたＤＶＤ－ＲＯＭの原盤（ディスク原盤）８が作成され、その原盤８を用いて、スタンパ９が作成される。そして、そのスタンパ９を用いて、多数のＤＶＤ－ＲＯＭ１０が製造される。

【００１５】なお、鍵発行センタ４とディスク製造業者７とは、異なる組織であっても、同一の組織であってもかまわない。また、図１では、ディスク製造業者７において、コンテンツを暗号化するようにしたが、コンテンツの暗号化も、鍵管理センタ４で行い、鍵管理センタ４から、ディスク製造業者７には、暗号化ディスクキーのセットおよび暗号化タイトルキーとともに、暗号化コンテンツを提供するようにすることが可能である。

【００１６】図２は、以上のようにして製造されるＤＶＤ－ＲＯＭ１０について、ＤＶＤ規格で規定されているディスクフォーマットを示している。

【００１７】図２（Ａ）に示すように、物理セクタ番号が０ｈ（ｈは、その前の数字が１６進数であることを表す）の物理セクタ（物理セクタ番号がｘの物理セクタを、以下、適宜、物理セクタ＃ｘと記述する）から、物理セクタ＃２ＦＦＦＦｈまでは、リードイン領域となっており、物理セクタ＃３００００ｈ以降が、コンテンツが記録されるメインデータ領域となっている。

【００１８】リードイン領域は、物理セクタ＃０ｈから＃２ＥＦＦＦｈまでが０の領域に、物理セクタ＃２Ｆ０００ｈから＃２Ｆ０１Ｆｈまでが参照用コードの領域に、物理セクタ＃２Ｆ０２０ｈから＃２Ｆ１ＦＦｈまでが０の領域に、物理セクタ＃２Ｆ２００ｈから＃２ＦＤＦＦｈまでがコントロールデータ領域に、物理セクタ＃２ＦＥ００ｈから＃２ＦＦＦＦｈまでが０の領域に、それぞれなっており、暗号化ディスクキーのセットは、コントロールデータ領域に記録される。

【００１９】即ち、コントロールデータ領域の先頭の物理セクタは、ディスク構造等の物理フォーマット情報が記録される領域に、２番目の物理セクタは、ディスク製造情報が記録される領域に、３番目から１６番目までの物理セクタは、コンテンツ供給者の情報が記録される領域に、それぞれなっており、それ以降のコントロールデータ領域は、その先頭から１６番目までの物理セクタと同様の領域が繰り返されるようになっている。そして、暗号化ディスクキーのセットは、以上のようなコントロールデータ領域のうちの、コンテンツ供給者の情報が記録される領域に記録される。

【００２０】メインデータ領域には、図２（Ｂ）に示すような２０６４バイト単位の論理セクタであるデータセクタが繰り返し配置されており、データセクタは、セクタ番号等のＩＤ(Identification)が配置される領域、ＩＤの誤り検出用データが配置される領域、コピー管理用データが配置される領域、ユーザデータが配置される領域、データセクタ全体の誤り検出用データが配置される領域から構成される。暗号化タイトルキーは、以上のようなデータセクタのうちの、コピー管理用データが配置される領域に記録される。

【００２１】なお、暗号化ディスクキーのセットが記録される領域、および暗号化タイトルキーが記録される領域は、いずれも、コンピュータの論理ファイルシステムを介して読み出せないようになっており、これにより、ディスクキーやタイトルキーが、ＤＶＤプレーヤの外部に漏れることを防止するようになっている。但し、暗号化ディスクキーのセットが記録される領域、および暗号化タイトルキーが記録される領域は、あくまでも、コンピュータの論理ファイルシステムを介して読み出せないだけで、ＤＶＤプレーヤの内部では、暗号化ディスクキーや暗号化タイトルキーが読み出され、暗号化タイトルキーや暗号化コンテンツの復号に用いられる。

【００２２】次に、図３は、図２に示したフォーマットのＤＶＤ－ＲＯＭ１０の再生を行う、従来（現行）のＤＶＤプレーヤの一例の構成を示している。

【００２３】ライセンスを受けたＤＶＤプレーヤは、そのＤＶＤプレーヤのメーカに割り当てられたマスタキー（以下、適宜、割り当てマスタキーという）を記憶しているマスタキー記憶部２１を有しており、復号器２２は、ＤＶＤ－ＲＯＭ１０に記録された暗号化ディスクキーのセットの中から、その割り当てマスタキーで暗号化されているものを読み出す。

【００２４】ここで、ＤＶＤ－ＲＯＭ１０に記録された暗号化ディスクキーのセットのうち、何番目のディスクキー（暗号化ディスクキー）が、ＤＶＤプレーヤのメーカに割り当てられているかに関する情報は、そのメーカに対して、ライセンス契約時に、マスタキーとともに与えられるようになっており、ＤＶＤプレーヤでは、その情報に基づいて、自身の割り当てマスタキーで暗号化されている暗号化ディスクキーが、ＤＶＤ－ＲＯＭ１０から読み出されるようになっている。

【００２５】復号器２２は、マスタキー記憶部２１に記憶されている割り当てマスタキーを読み出し、ＤＶＤ－ＲＯＭ１０から読み出した暗号化ディスクキーを、割り当てマスタキーで復号する。そして、復号器２２は、その復号の結果得られるディスクキーを、復号器２３に供給する。

【００２６】復号器２３は、ＤＶＤ－ＲＯＭ１０におけるデータセクタのコピー管理用データ領域に記録されている暗号化タイトルキーを読み出し、その暗号化タイトルキーを、復号器２２からのディスクキーで復号する。そして、復号器２３は、その復号の結果得られるタイト

7

ルキーを、復号器２４に供給する。

【００２７】復号器２４は、ＤＶＤ－ＲＯＭ１０におけるデータセクタのユーザデータ領域に記録されている暗号化コンテンツを読み出し、その暗号化コンテンツを、復号器２３からのタイトルキーで復号する。復号器２４による復号の結果得られるディジタルデータのコンテンツ（いわゆる平文とされたコンテンツ）は、Ａ／Ｄ(Analog/Digital)変換され、アナログ信号とされて、外部に出力される。

【００２８】なお、上述したコンテンツスクランブルシステムについては、例えば、「日経エレクトロニクス」、１９９７年８月１８日（ｎｏ．６９６）、ｐｐ．１１０－１１９、日経ＢＰ社等に、その詳細が記載されている。

【００２９】

【発明が解決しようとする課題】以上のような、ＤＶＤ－ＲＯＭで採用されているコンテンツスクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ＲＯＭメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、ＲＡＭメディアという）への適用については考慮されていない。

【００３０】即ち、ＲＡＭメディアである、例えば、ＤＶＤ－ＲＡＭに、コンテンツスクランブルシステムを採用するには、そのＤＶＤ－ＲＡＭに記録するコンテンツのコンテンツ供給者によって発行されるタイトルキーやディスクキーが必要となるが、将来、どのようなコンテンツが記録されるか分からないＤＶＤ－ＲＡＭについて、コンテンツ供給者が、タイトルキーやディスクキーを発行するのは困難である（コンテンツ供給者が、どのようなコンテンツが記録されるか分からないＤＶＤ－ＲＡＭに対して、タイトルキーやディスクキーを決めることはできない）。

【００３１】そこで、ＤＶＤ－ＲＡＭ等のＲＡＭメディアについては、コンテンツスクランブルシステムとは異なる方法で、違法コピーを防止するようにすることも可能であるが、この場合、そのような異なる方法が採用たＤＶＤ－ＲＡＭを、現行のＤＶＤプレーヤで再生することはできなくなる。従って、コンテンツスクランブルシステムとは異なる方法をＤＶＤ－ＲＡＭに採用した場合には、そのようなＤＶＤ－ＲＡＭに対応したＤＶＤプレーヤを、現行のＤＶＤプレーヤを有するユーザに新たに購入してもらわなければならなくなるため、コンテンツスクランブルシステムとは異なる方法を、ＲＡＭメディアに採用するのは好ましくない。

【００３２】本発明は、このような状況に鑑みてなされたものであり、ＲＡＭメディアに対する違法コピーを防止するとともに、適法なコピーが行われたＲＡＭメディアを、現行のプレーヤで再生することができるようにするものである。

8

【００３３】

【課題を解決するための手段】本発明のデータ提供装置は、第１キーで暗号化された第２キーである暗号化第２キーを取得する取得手段と、暗号化第２キーを、第１キーに基づいて復号する暗号化第２キー復号手段と、暗号化第２キー復号手段により復号された第２キーを利用して、データを暗号化する暗号化手段と、暗号化手段により暗号化されたデータである暗号化データを提供する提供手段とを含むことを特徴とする。

【００３４】暗号化手段には、第３キーを、第２キーで暗号化し、暗号化第３キーを出力する第３キー暗号化手段と、データを、第３キーで暗号化するデータ暗号化手段とを設けることができ、この場合、提供手段には、暗号化データを、暗号化第３キーとともに提供させることができる。

【００３５】データ提供装置には、第１キーを記憶している記憶手段をさらに設けることができる。

【００３６】取得手段には、複数の第１キーそれぞれで暗号化された第２キーである暗号化第２キーのセットのうち、記憶手段に記憶されている第１キーで復号可能なものを取得させることができる。

【００３７】暗号化第２キー復号手段による復号方法、および暗号化手段による暗号化方法は、ＤＶＤ(Digital Versatile Disc)規格に準拠したものとすることができる。

【００３８】取得手段には、データ記録媒体に記録された暗号化第２キーを読み出させることができる。また、取得手段には、伝送路を介して伝送されてくる暗号化第２キーを受信させることができる。

【００３９】提供手段には、暗号化データを、データ記録媒体に記録させることができる。また、提供手段には、暗号化データを、伝送路を介して伝送させることができる。

【００４０】本発明のデータ提供方法は、第１キーで暗号化された第２キーである暗号化第２キーを取得する取得ステップと、暗号化第２キーを、第１キーに基づいて復号する暗号化第２キー復号ステップと、暗号化第２キー復号ステップにおいて復号された第２キーを利用して、データを暗号化する暗号化ステップと、暗号化ステップにおいて暗号化されたデータである暗号化データを提供する提供ステップとを含むことを特徴とする。

【００４１】本発明のプログラム記録媒体は、第１キーで暗号化された第２キーである暗号化第２キーを取得する取得ステップと、暗号化第２キーを、第１キーに基づいて復号する暗号化第２キー復号ステップと、暗号化第２キー復号ステップにおいて復号された第２キーを利用して、データを暗号化する暗号化ステップと、暗号化ステップにおいて暗号化されたデータである暗号化データを提供する提供ステップとを含むプログラムが記録されていることを特徴とする。

9

【００４２】本発明のデータ記録媒体は、第１キーで暗号化された第２キーである暗号化第２キーが記録されており、後に、暗号化第２キーを、第１キーで復号し、第２キーを得て、その第２キーを利用して、データが暗号化されて記録されることを特徴とする。

【００４３】このデータ記録媒体は、ＤＶＤ(Digital Versatile Disc)規格に準拠したフォーマットを有するものとすることができる。

【００４４】また、このデータ記録媒体は、複数の第１キーそれぞれで暗号化された第２キーである暗号化第２キーのセットが記録されているものとすることができる。

【００４５】暗号化第２キーは、読み出しが可能であるが、書き込みが不可能な記録領域に記録しておくようにすることができる。

【００４６】本発明のデータ記録媒体の製造方法は、後に、第１キーで暗号化された第２キーである暗号化第２キーを、第１キーで復号し、第２キーを得て、その第２キーを利用して、データが暗号化されて記録されるデータ記録媒体に、暗号化第２キーを記録することを特徴とする。

【００４７】本発明のデータ提供装置およびデータ提供方法、並びにプログラム記録媒体においては、第１キーで暗号化された第２キーである暗号化第２キーが取得され、暗号化第２キーが、第１キーに基づいて復号される。そして、その復号された第２キーを利用して、データが暗号化され、その暗号化されたデータである暗号化データが提供される。

【００４８】本発明のデータ記録媒体においては、第１キーで暗号化された第２キーである暗号化第２キーが記録されており、後に、暗号化第２キーが、第１キーで復号され、その結果得られる第２キーを利用して、データが暗号化されて記録される。

【００４９】本発明のデータ記録媒体の製造方法においては、後に、第１キーで暗号化された第２キーである暗号化第２キーを、第１キーで復号し、第２キーを得て、その第２キーを利用して、データが暗号化されて記録されるデータ記録媒体に、暗号化第２キーが記録される。

【００５０】

【発明の実施の形態】図４は、本発明を適用したＲＡＭメディアであるＤＶＤ－ＲＡＭの製造工程の一実施の形態を示している。

【００５１】ＤＶＤ－ＲＡＭの製造は、図４に示すように、鍵管理センタ３１およびディスク製造業者３３によって行われる。

【００５２】即ち、鍵管理センタ３１では、図５のフローチャートに示すように、まず最初に、ステップＳ１において、ＤＶＤ－ＲＡＭに用いる適当なディスクキー（第２キー）が決定され、ステップＳ２に進み、図１の鍵管理センタ４における場合と同様に、ＤＶＤ規格に準

10

拠した暗号化を行う暗号化器３２によって、ディスクキーを、複数のマスタキー（第１キー）それぞれで暗号化することにより、暗号化ディスクキーのセットが作成される。鍵管理センタ３１で作成された暗号化ディスクキーのセットは、ステップ３において、ディスク製造業者３３に提供される。

【００５３】なお、鍵管理センタ３１は、ライセンス契約を行ったメーカそれぞれに対して、異なるマスタキーを割り当てる。鍵管理センタ３１は、ディスクキーの暗号化に用いる複数のマスタキーとして、十分な数のマスタキーを用意しており（従って、ディスクキーは、そのような十分な数のマスタキーそれぞれで暗号化される）、これにより、ライセンス契約を行うメーカの数が増加しても、各メーカに、異なるマスタキーを割り当てることができるようになっている。

【００５４】ディスク製造業者３３では、図６のフローチャートに示すように、まず最初に、ステップＳ１１において、鍵管理センタ３１から提供される暗号化ディスクキーのセットが取得され、ステップＳ１２に進み、その暗号化ディスクキーのセットが記録された、ＤＶＤ規格に準拠したフォーマットのＤＶＤ－ＲＡＭの原盤（ディスク原盤）３４が作成される。即ち、ディスク製造業者３３においては、ステップＳ１２において、前述の図２に示したようなフォーマットを有するＤＶＤ－ＲＡＭの原盤３４であって、そのリードイン領域のコントロールデータ領域に、暗号化ディスクキーのセットが記録されたものが作成される。さらに、ディスク製造業者３３では、ステップＳ１３において、原盤３４を用いて、スタンパ３５が作成され、ステップＳ１４に進み、そのスタンパ３５を用いて、多数のＤＶＤ－ＲＡＭ３６が製造（スタンプ）される。

【００５５】以上のようにして、図２に示したＤＶＤ規格に規定されているフォーマットのＤＶＤ－ＲＡＭ３６が製造される。

【００５６】なお、ＤＶＤ－ＲＡＭ３６は、上述のように、スタンパ３５を用いてスタンプが行われることにより製造されるから、暗号化ディスクキーのセットが記録される記録領域（リードイン領域のコントロールデータ領域（図２（Ａ））は、読み出しは可能であるが、書き込みが不可能な領域となる。

【００５７】ここで、違法コピーを、より強固に防止するため、鍵管理センタ３１においては、ディスクキーを頻繁に更新するようにし、できるだけ、異なるディスクキー（暗号化ディスクキー）が記録されたＤＶＤ－ＲＡＭが製造されるようにするのが望ましい。

【００５８】また、鍵発行センタ３１とディスク製造業者３３とは、異なる組織であっても、同一の組織であってもかまわない。

【００５９】次に、図７は、図４乃至図６で説明したようにして製造されたＤＶＤ－ＲＡＭ３６に対して、ディ

ジタルデータのコンテンツを記録するＤＶＤレコーダの一実施の形態の構成例を示している。

【００６０】マスタキー記憶部４１は、ＤＶＤレコーダ（のＬＳＩやソフトウェアモジュール）のメーカに割り当てられたマスタキー（割り当てマスタキー）を記憶している。

【００６１】復号器４２は、ＤＶＤ－ＲＡＭ３６のリードイン領域に記録された暗号化ディスクキーのセットの中から、割り当てマスタキーで暗号化されたものを読み出し（取得し）、マスタキー記憶部４１に記憶されているマスタキーで、ＤＶＤ規格に準拠した復号方法（復号アルゴリズム）により復号するようになっている。復号器４２による復号の結果得られるディスクキーは、暗号化器４３に供給されるようになっている。

【００６２】暗号化器４３は、タイトルキー生成部４４から供給されるタイトルキーを、復号器４２から供給されるディスクキーで、ＤＶＤ規格に準拠した暗号化方法（暗号化アルゴリズム）により暗号化し、その結果得られる暗号化タイトルキーを、ＤＶＤ－ＲＡＭ３６におけるデータセクタ（図２（Ｂ））のコピー管理用データ領域に記録（提供）するようになっている。

【００６３】タイトルキー生成部４４は、タイトルキー（第３キー）として用いることのできるキーを、例えば、乱数等を利用して生成し、暗号化器４３および４５に供給するようになっている。

【００６４】暗号化器４５は、ＤＶＤ－ＲＡＭ３６に記録しようとするコンテンツとしてのディジタルデータを受信し、そのコンテンツを、タイトルキー生成部４４から供給されるタイトルキーで、ＤＶＤ規格に準拠した暗号化方法により暗号化するようになっている。さらに、暗号化器４５は、その暗号化の結果得られる暗号化コンテンツを、ＤＶＤ－ＲＡＭ３６におけるデータセクタのユーザデータ領域に記録するようになっている。

【００６５】以上のように構成されるＤＶＤレコーダでは、図８のフローチャートに示すようにして、ＤＶＤ－ＲＡＭ３６へのコンテンツの記録が行われる。

【００６６】即ち、まず最初に、ステップＳ２１において、復号器４２は、ＤＶＤ－ＲＡＭ３６のリードイン領域に記録された暗号化ディスクキーのセットの中から、割り当てマスタキーで暗号化されたものを読み出し、ステップＳ２２に進み、マスタキー記憶部４１に記憶されているマスタキーで復号して、ディスクキーを得る。このディスクキーは、復号部４２から暗号化器４３に供給される。

【００６７】そして、ステップＳ２３に進み、タイトルキー生成部４４において、タイトルキーが生成され、暗号化器４３および４５に供給される。暗号化器４３は、ステップＳ２４において、タイトルキー生成部４４から供給されるタイトルキーを、復号器４２から供給されるディスクキーで暗号化し、その結果得られる暗号化タイトルキーを、ＤＶＤ－ＲＡＭ３６に記録する。

【００６８】その後、ＤＶＤ－ＲＡＭ３６に記録すべきコンテンツが、暗号化器４５に入力されると、暗号化器４５は、ステップＳ２５において、そのコンテンツを受信し、ステップＳ２６に進み、そのコンテンツを、タイトルキー生成部４４からのタイトルキーで暗号化し、ＤＶＤ－ＲＡＭ３６に記録する。そして、ステップＳ２７に進み、記録対象のコンテンツを、すべて記録したかどうかが判定され、まだ記録していないと判定された場合、暗号化器４５に、次のコンテンツが入力されるのを待って、ステップＳ２５に戻り、以下、同様の処理を繰り返す。

【００６９】また、ステップＳ２７において、記録対象のコンテンツを、すべて記録したと判定された場合、処理を終了する。

【００７０】以上のようにして、コンテンツが記録されたＤＶＤ－ＲＡＭ３６には、図１で説明したようにして製造されるＤＶＤ－ＲＯＭ１０と同一フォーマットで、暗号化ディスクキーのセット、暗号化タイトルキー、および暗号化コンテンツが記録されている。従って、ＤＶＤ－ＲＡＭ３６は、マスタキーを有していないＤＶＤプレーヤでは再生することができないので、不正なコピーを防止することができ、さらに、ＤＶＤ－ＲＯＭ１０を再生する図３のＤＶＤプレーヤと同一のＤＶＤプレーヤで再生することができる。即ち、ＤＶＤ－ＲＡＭに対する違法コピーを防止するとともに、適法なコピーが行われたＤＶＤ－ＲＡＭを、現行のＤＶＤプレーヤで再生することができる。

【００７１】次に、図９は、ＤＶＤ－ＲＡＭ３６を再生するＤＶＤプレーヤの構成例を示している。

【００７２】図９におけるマスタキー記憶部５１、または復号器５２乃至５４は、図３におけるマスタキー記憶部２１、または復号器２２乃至２４とそれぞれ同様に構成されており、従って、図９のＤＶＤプレーヤでは、図３におけるＤＶＤプレーヤがＤＶＤ－ＲＯＭ１０を再生するのと同様にして、ＤＶＤ－ＲＡＭ３６が再生される。

【００７３】即ち、図９のＤＶＤプレーヤでは、図１０のフローチャートに示すように、まず最初に、ステップＳ３１において、復号器５２は、ＤＶＤ－ＲＡＭ３６のリードイン領域に記録された暗号化ディスクキーのセットの中から、マスタキー記憶部５１に記憶されている割り当てマスタキーで暗号化されているものを読み出す。さらに、復号器５２は、ステップＳ３２において、マスタキー記憶部５１に記憶されている割り当てマスタキーを読み出し、ＤＶＤ－ＲＡＭ３６から読み出した暗号化ディスクキーを、割り当てマスタキーで復号する。そして、復号器５２は、その復号の結果得られるディスクキーを、復号器５３に供給する。

【００７４】復号器５３は、ステップＳ３３において、

13

ＤＶＤ－ＲＡＭ３６におけるデータセクタのコピー管理用データ領域に記録されている暗号化タイトルキーを読み出し、ステップＳ３４に進み、その暗号化タイトルキーを、復号器５２からのディスクキーで復号する。そして、復号器５３は、その復号の結果得られるタイトルキーを、復号器５４に供給する。

【００７５】復号器５４は、ステップＳ３５において、ＤＶＤ－ＲＡＭ３６におけるデータセクタのユーザデータ領域に記録されている暗号化コンテンツを読み出し、ステップＳ３６に進み、その暗号化コンテンツを、復号器５３からのタイトルキーで復号する。復号器５４による復号の結果得られるディジタルデータのコンテンツ（いわゆる平文とされたコンテンツ）は、Ａ／Ｄ(Analog/Digital)変換され、アナログ信号とされて、外部に出力される。

【００７６】そして、ステップＳ３７に進み、再生対象のコンテンツを、すべて再生したかどうかが判定され、まだ再生していないと判定された場合、ステップＳ３５に戻り、次に再生すべき暗号化コンテンツを、ＤＶＤ－ＲＡＭ３６から読み出し、以下、同様の処理を繰り返す。

【００７７】また、ステップＳ３７において、再生対象のコンテンツを、すべて再生したと判定された場合、処理を終了する。

【００７８】以上のように、ＤＶＤ－ＲＡＭ３６は、図３のＤＶＤプレーヤと同一構成の図９のＤＶＤプレーヤによって再生することができる。

【００７９】なお、ＤＶＤレコーダのマスタキー記憶部４１や、ＤＶＤプレーヤのマスタキー記憶部５１に記憶されているマスタキーが、違法なコピーを行おうとする者（以下、適宜、違法者という）によって入手され、ライセンス契約を受けずに、図９（あるいは図３）に示したＤＶＤプレーヤと同一構成のＤＶＤプレーヤが製造されると、違法なコピーを行うことが可能となる。しかしながら、この場合、図４の鍵管理センタ３１において、違法者が入手したマスタキーでディスクキーを暗号化した暗号化ディスクキー（以下、違法ディスクキーという）を、ＤＶＤ－ＲＡＭ３６に記録する暗号化ディスクキーのセットから削除する（例えば、違法ディスクキーを、暗号化ディスクキーとしては用いられないオール０とする）ことにより、違法者によって入手されたマスタキーを有するＤＶＤプレーヤにおけるＤＶＤ－ＲＡＭ３６の再生を不可能にすることができ、これにより、違法者による違法なコピーによる被害の拡大を防止することができる。

【００８０】但し、この場合、違法者によって入手された違法ディスクキーが割り当てられていたメーカには、新たなディスクキー（まだ、メーカに割り当てられていないディスクキーのうちの１つ）を割り当てる必要がある。

14

【００８１】次に、図７のＤＶＤレコーダにおいては、ＤＶＤ－ＲＡＭ３６に記録された暗号化ディスクキーを復号して得たディスクキーを利用して、コンテンツを暗号化し、ＤＶＤ－ＲＡＭ３６に記録するようにしたが、暗号化したコンテンツは、ＤＶＤ－ＲＡＭ３６に記録する他、伝送路を介して、遠方の装置（例えば、ＤＶＤプレーヤ）に伝送（提供）するようにすることも可能である。

【００８２】図１１は、そのようなＤＶＤレコーダの構成例を示している。なお、図中、図７における場合と対応する部分については、同一の符号を付してある。即ち、図１１のＤＶＤレコーダは、図７における場合と基本的に同様に構成されている。

【００８３】図１１のＤＶＤレコーダでは、図１２のフローチャートに示すように、まず最初に、復号器４２は、ステップＳ４１において、ＤＶＤ－ＲＡＭ３６のリードイン領域に記録された暗号化ディスクキーのセットの中から、割り当てマスタキーで暗号化されたものを読み出し、ステップＳ４２に進み、マスタキー記憶部４１に記憶されているマスタキーで復号して、ディスクキーを得る。このディスクキーは、復号部４２から暗号化器４３に供給される。

【００８４】そして、ステップＳ４３に進み、タイトルキー生成部４４において、タイトルキーが生成され、暗号化器４３に供給される。暗号化器４３は、ステップＳ４４において、タイトルキー生成部４４から供給されるタイトルキーを、復号器４２から供給されるディスクキーで暗号化する。さらに、ステップＳ４４では、暗号化器４３による結果得られる暗号化タイトルキーが、ステップＳ４１でＤＶＤ－ＲＡＭ３６から読み出された暗号化ディスクキーのセットとともに、伝送路を介して伝送（提供）される。

【００８５】その後、伝送すべきコンテンツが、暗号化器４５に入力されると、暗号化器４５は、ステップＳ４５において、そのコンテンツを受信し、ステップＳ４６に進み、そのコンテンツを、タイトルキー生成部４４からのタイトルキーで暗号化し、伝送路を介して伝送する。そして、ステップＳ４７に進み、伝送対象のコンテンツを、すべて伝送したかどうかが判定され、まだ伝送していないと判定された場合、暗号化器４５に、次のコンテンツが入力されるのを待って、ステップＳ４５に戻り、以下、同様の処理を繰り返す。

【００８６】また、ステップＳ４７において、伝送対象のコンテンツを、すべて伝送したと判定された場合、処理を終了する。

【００８７】以上のようにして伝送される暗号化ディスクキーのセット、暗号化タイトルキー、および暗号化コンテンツを受信した受信側では、図９に示したＤＶＤプレーヤによって、コンテンツを再生することができる。

【００８８】即ち、この場合、図９のＤＶＤプレーヤで

は、図１３のフローチャートに示すように、まず最初に、ステップＳ５１において、伝送路を介して伝送されてくる、暗号化ディスクキーのセットが受信され、ステップＳ５２に進み、復号器５２は、その暗号化ディスクキーのセットの中から、マスタキー記憶部５１に記憶されている割り当てマスタキーで暗号化されているものを抽出する。さらに、復号器５２は、ステップＳ５２において、マスタキー記憶部５１に記憶されている割り当てマスタキーを読み出し、暗号化ディスクキーのセットの中から抽出した暗号化ディスクキーを、割り当てマスタキーで復号する。そして、復号器５２は、その復号の結果得られるディスクキーを、復号器５３に供給する。

【００８９】復号器５３は、ステップＳ５３において、伝送路を介して伝送されてくる暗号化タイトルキーを受信し、ステップＳ５４に進み、その暗号化タイトルキーを、復号器５２からのディスクキーで復号する。そして、復号器５３は、その復号の結果得られるタイトルキーを、復号器５４に供給する。

【００９０】復号器５４は、ステップＳ５５において、伝送路を介して伝送されてくる暗号化コンテンツを受信し、ステップＳ５６に進み、その暗号化コンテンツを、復号器５３からのタイトルキーで復号する。復号器５４による復号の結果得られるディジタルデータのコンテンツは、Ａ／Ｄ(Analog/Digital)変換され、アナログ信号とされて、外部に出力される。

【００９１】そして、ステップＳ５７に進み、受信対象のコンテンツを、すべて受信したかどうかが判定され、まだ受信していないと判定された場合、ステップＳ５５に戻り、次に伝送されてくる暗号化コンテンツが受信され、以下、同様の処理が繰り返される。

【００９２】また、ステップＳ５７において、受信対象のコンテンツを、すべて受信したと判定された場合、処理を終了する。

【００９３】なお、上述の場合には、ＤＶＤデコーダからＤＶＤプレーヤに対して、暗号化ディスクキーのセット、暗号化タイトルキー、および暗号化コンテンツを伝送するようにしたが、ＤＶＤレコーダからＤＶＤプレーヤに対しては、暗号化タイトルキーと暗号化コンテンツを伝送し、ＤＶＤプレーヤにおいて、その割り当てマスタキーで暗号化された暗号化ディスクキーを、鍵管理センタ３１から取得して、コンテンツを再生するようにすることも可能である。

【００９４】次に、暗号化ディスクキーのセットは、ＤＶＤ－ＲＡＭ３６に記録しておくのではなく、例えば、鍵管理センタ３１などから、伝送路を介して、ＤＶＤレコーダに伝送し、ＤＶＤレコーダでは、伝送路を介して伝送されてくる暗号化ディスクキーのセットを受信し（取得し）、これを利用して、コンテンツを暗号化して、ＤＶＤ－ＲＡＭ３６に記録することで、ＤＶＤ－ＲＯＭ１０と同一フォーマットのＤＶＤ－ＲＡＭ３６を作成するようにすることが可能である。

【００９５】図１４は、そのようなＤＶＤレコーダの構成例を示している。なお、図中、図７における場合と対応する部分については、同一の符号を付してある。即ち、図１４のＤＶＤレコーダは、図７における場合と基本的に同様に構成されている。

【００９６】図１４のＤＶＤレコーダでは、図１５のフローチャートに示すように、まず最初に、ステップＳ６１において、復号器４２は、伝送路を介して伝送されてくる暗号化ディスクキーのセットを受信し、ステップＳ６２に進む。ステップＳ６２では、復号器４２で受信された暗号化ディスクキーのセットが、ＤＶＤ－ＲＡＭ３６のリードイン領域に記録され、ステップＳ６３に進む。

【００９７】ステップＳ６３では、復号器４２は、ステップＳ６１で受信した暗号化ディスクキーの中から、割り当てマスタキーで暗号化されたものを抽出し、マスタキー記憶部４１に記憶されている割り当てマスタキーで復号して、ディスクキーを得る。このディスクキーは、復号部４２から暗号化器４３に供給される。

【００９８】そして、ステップＳ６４に進み、以下、ステップＳ６４乃至Ｓ６８において、図８のステップＳ２３乃至Ｓ２７における場合とそれぞれ同様の処理が行われ、処理を終了する。

【００９９】以上の処理により、図１４のＤＶＤレコーダにおいても、図９のＤＶＤプレーヤで再生可能なＤＶＤ－ＲＡＭ３６を得ることができる。

【０１００】即ち、図１４のＤＶＤレコーダによってコンテンツが記録されたＤＶＤ－ＲＡＭ３６は、図９に示したＤＶＤプレーヤにおいて、図１０のフローチャートにしたがった処理が行われることにより再生することができる。

【０１０１】次に、暗号化ディスクキーのセットは、例えば、鍵管理センタ３１などから、伝送路を介して、ＤＶＤレコーダに伝送し、ＤＶＤレコーダでは、伝送路を介して伝送されてくる暗号化ディスクキーのセットを受信し（取得し）、これを利用して、コンテンツを暗号化し、さらに、その結果得られる暗号化コンテンツを、伝送路を介して、例えば、ＤＶＤプレーヤなどの遠方の装置に伝送（提供）するようにすることも可能である。

【０１０２】図１６は、そのようなＤＶＤレコーダの構成例を示している。なお、図中、図７における場合と対応する部分については、同一の符号を付してある。即ち、図１６のＤＶＤレコーダは、図７における場合と基本的に同様に構成されている。

【０１０３】図１６のＤＶＤレコーダでは、図１７のフローチャートに示すように、まず最初に、ステップＳ７１において、復号器４２は、伝送路を介して伝送されてくる暗号化ディスクキーのセットを受信し、ステップＳ７２に進む。ステップＳ７２では、復号器４２で受信さ

れた暗号化ディスクキーのセットが、伝送路を介して伝送され、ステップＳ７３に進む。

【０１０４】ステップＳ７３では、復号器４２は、ステップＳ７１で受信した暗号化ディスクキーの中から、割り当てマスタキーで暗号化されたものを抽出し、マスタキー記憶部４１に記憶されているマスタキーで復号して、ディスクキーを得る。このディスクキーは、復号部４２から暗号化器４３に供給される。

【０１０５】そして、ステップＳ７４に進み、タイトルキー生成部４４において、タイトルキーが生成され、暗号化器４３に供給される。暗号化器４３は、ステップＳ７５において、タイトルキー生成部４４から供給されるタイトルキーを、復号器４２から供給されるディスクキーで暗号化し、その結果得られる暗号化タイトルキーを、伝送路を介して伝送（提供）する。

【０１０６】その後、ステップＳ７６に進み、以下、ステップＳ７６乃至Ｓ７８において、図１２のステップＳ４５乃至Ｓ４７における場合とそれぞれ同様の処理が行われ、処理を終了する。

【０１０７】以上のようにして伝送される暗号化ディスクキーのセット、暗号化タイトルキー、および暗号化コンテンツを受信した受信側では、図９に示したＤＶＤプレーヤによって、図１３のフローチャートにしたがった処理が行われることにより、コンテンツを再生することができる。

【０１０８】次に、ＤＶＤプレーヤにおいて、暗号化ディスクキーのセットを、ＤＶＤレコーダに提供し、ＤＶＤレコーダにおいて、その暗号化ディスクキーのセットを利用して、コンテンツを暗号化し、ＤＶＤプレーヤに提供して、ＤＶＤプレーヤでは、ＤＶＤレコーダに提供した暗号化ディスクキーのセットを利用して、ＤＶＤレコーダから提供される暗号化コンテンツを再生することが可能である。

【０１０９】図１８は、そのようなＤＶＤレコーダとＤＶＤプレーヤからなるＤＶＤシステムの構成例を示している。

【０１１０】図１８のＤＶＤシステムは、ＤＶＤレコーダ６１とＤＶＤプレーヤ６２とから構成されており、ＤＶＤレコーダ６１は、図１６に示したように構成され、そこでは、図１７のフローチャートにしたがった処理が行われる。

【０１１１】一方、ＤＶＤプレーヤ６２は、例えば、図９に示したように構成され、そこでは、図１９に示すフローチャートにしたがった処理が行われる。

【０１１２】即ち、ＤＶＤプレーヤ６２では、まず最初に、ステップＳ８１において、例えば、ＤＶＤ－ＲＡＭ３６に記録された暗号化ディスクキーのセットが読み出され、あるいは、鍵管理センタ３１などから伝送路を介して伝送されてくる暗号化ディスクキーのセットが受信され、その暗号化ディスクキーのセットが、伝送路を介して、ＤＶＤレコーダ６１に伝送される。

【０１１３】そして、ステップＳ８２に進み、復号器５２は、ＤＶＤレコーダ６１に伝送された暗号化ディスクキーのセットの中から、マスタキー記憶部５１に記憶されている割り当てマスタキーで暗号化されているものを抽出する。さらに、復号器５２は、ステップＳ８２において、マスタキー記憶部５１に記憶されている割り当てマスタキーを読み出し、暗号化ディスクキーのセットの中から抽出した暗号化ディスクキーを、割り当てマスタキーで復号する。そして、復号器５２は、その復号の結果得られるディスクキーを、復号器５３に供給する。

【０１１４】復号器５３は、ステップＳ８３において、ＤＶＤレコーダ６１から、伝送路を介して伝送されてくる暗号化タイトルキーを受信し、ステップＳ８４に進み、その暗号化タイトルキーを、復号器５２からのディスクキーで復号する。そして、復号器５３は、その復号の結果得られるタイトルキーを、復号器５４に供給する。

【０１１５】復号器５４は、ステップＳ８５において、ＤＶＤレコーダ６１から、伝送路を介して伝送されてくる暗号化コンテンツを受信し、ステップＳ８６に進み、その暗号化コンテンツを、復号器５３からのタイトルキーで復号する。復号器５４による復号の結果得られるディジタルデータのコンテンツは、Ａ／Ｄ(Analog/Digital)変換され、アナログ信号とされて、外部に出力される。

【０１１６】そして、ステップＳ８７に進み、受信対象のコンテンツを、すべて受信したかどうかが判定され、まだ受信していないと判定された場合、ステップＳ８５に戻り、ＤＶＤレコーダ６１から、次に伝送されてくる暗号化コンテンツを受信し、以下、同様の処理を繰り返す。

【０１１７】また、ステップＳ８７において、受信対象のコンテンツを、すべて受信したと判定された場合、処理を終了する。

【０１１８】次に、上述した一連の処理は、ハードウェアにより行うこともできるし、ソフトウェアにより行うこともできる。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアとしてのＤＶＤレコーダやＤＶＤプレーヤに組み込まれているコンピュータや、汎用のコンピュータ等にインストールされる。

【０１１９】そこで、図２０を参照して、上述した一連の処理を実行するプログラムをコンピュータにインストールし、コンピュータによって実行可能な状態とするために用いられる、そのプログラムが記録されているプログラム記録媒体について説明する。

【０１２０】プログラムは、図２０（Ａ）に示すように、コンピュータ１０１に内蔵されている記録媒体としてのハードディスク１０２や半導体メモリ１０３に予め

記録しておくことができる。

【０１２１】あるいはまた、プログラムは、図２０（Ｂ）に示すように、フロッピー（登録商標）ディスク１１１、CD-ROM(Compact Disc Read Only Memory)１１２，MO(Magneto optical)ディスク１１３，DVD(Digital Versatile Disc)１１４、磁気ディスク１１５、半導体メモリ１１６などの記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このような記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０１２２】なお、プログラムは、上述したような記録媒体からコンピュータにインストールする他、図２０（Ｃ）に示すように、ダウンロードサイト１２１から、ディジタル衛星放送用の人工衛星１２２を介して、コンピュータ１０１に無線で転送したり、LAN(Local Area Network)、インターネットといったネットワーク１３１を介して、コンピュータ１２３に有線で転送し、コンピュータ１０１において、内蔵するハードディスク１０２などにインストールすることができる。

【０１２３】また、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【０１２４】次に、図２１は、図２０のコンピュータ１０１の構成例を示している。

【０１２５】コンピュータ１０１は、図２１に示すように、CPU(Central Processing Unit)１４２を内蔵している。CPU１４２には、バス１４１を介して、入出力インタフェース１４５が接続されており、CPU１４２は、入出力インタフェース１４５を介して、ユーザによって、キーボードやマウス等で構成される入力部１４７が操作されることにより指令が入力されると、それにしたがって、図２０（Ａ）の半導体メモリ１０３に対応するROM(Read Only Memory)１４３に格納されているプログラムを実行する。あるいは、また、CPU１４２は、ハードディスク１０２に格納されているプログラム、衛星１２２若しくはネットワーク１３１から転送され、通信部１４８で受信されてハードディスク１０２にインストールされたプログラム、またはドライブ１４９に装着されたフロッピディスク１１１、CD-ROM１１２、MOディスク１１３、DVD１１４、若しくは磁気ディスク１１５から読み出されてハードディスク１０２にインストールされたプログラムを、RAM(Random Access Memory)１４４にロードして実行する。そして、CPU１４２は、その処理結果を、例えば、入出力インタフェース１４５を介して、LCD(Liquid CryStal Display)等で構成される表示部１４６に、必要に応じて出力する。

【０１２６】なお、本実施の形態では、ＲＡＭメディアとして、ＤＶＤ－ＲＡＭを用いた場合について説明したが、本発明は、ＤＶＤ－ＲＡＭ以外の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ等のＲＡＭメディアにも適用可能である。

【０１２７】さらに、本実施の形態では、ディスクキーで暗号化されるタイトルキーで、コンテンツを暗号化するようにしたが、コンテンツの暗号化は、タイトルキーを用いずに、ディスクキーで行うようにすることも可能である。

【０１２８】また、ＤＶＤ－ＲＡＭ３６には、画像や音声のデータの他、コンピュータによって実行されるプログラム等を記録することが可能である。

【０１２９】

【発明の効果】本発明のデータ提供装置およびデータ提供方法、並びにプログラム記録媒体によれば、第１キーで暗号化された第２キーである暗号化第２キーが取得され、暗号化第２キーが、第１キーに基づいて復号される。そして、その復号された第２キーを利用して、データが暗号化され、その暗号化されたデータである暗号化データが提供される。従って、第１キーで暗号化される第２キーを利用して暗号化したデータを得ることができる。

【０１３０】本発明のデータ記録媒体によれば、第１キーで暗号化された第２キーである暗号化第２キーが記録されており、後に、暗号化第２キーが、第１キーで復号され、その結果得られる第２キーを利用して、データが暗号化されて記録される。従って、第１キーで暗号化される第２キーを利用して暗号化したデータを記録することができる。

【０１３１】本発明のデータ記録媒体の製造方法によれば、後に、第１キーで暗号化された第２キーである暗号化第２キーを、第１キーで復号し、第２キーを得て、その第２キーを利用して、データが暗号化されて記録されるデータ記録媒体に、暗号化第２キーが記録される。従って、第１キーで暗号化される第２キーを利用して暗号化したデータを記録することのできるデータ記録媒体を製造することができる。

【図面の簡単な説明】

【図１】ＤＶＤ－ＲＯＭの製造工程を説明するための図である。

【図２】ＤＶＤ規格のディスクフォーマットを示す図である。

【図３】従来のＤＶＤプレーヤの一例の構成例を示すブロック図である。

【図４】本発明を適用したＤＶＤ－ＲＡＭの製造工程を説明するための図である。

【図５】図４の鍵管理センタ３１における処理を説明するためのフローチャートである。

【図６】図４のディスク製造業者３３における処理を説明するためのフローチャートである。

21

【図７】本発明を適用したＤＶＤレコーダの第１実施の形態の構成例を示すブロック図である。

【図８】図７のＤＶＤレコーダの処理を説明するためのフローチャートである。

【図９】コンテンツを再生するＤＶＤプレーヤの構成例を示すブロック図である。

【図１０】図７のＤＶＤレコーダによってコンテンツが記録されたＤＶＤ－ＲＡＭを再生する場合の、図９のＤＶＤプレーヤの処理を説明するためのフローチャートである。

【図１１】本発明を適用したＤＶＤレコーダの第２実施の形態の構成例を示すブロック図である。

【図１２】図１１のＤＶＤレコーダの処理を説明するためのフローチャートである。

【図１３】図１１のＤＶＤレコーダから送信されてくるコンテンツを再生する場合の、図９のＤＶＤプレーヤの処理を説明するためのフローチャートである。

【図１４】本発明を適用したＤＶＤレコーダの第３実施の形態の構成例を示すブロック図である。

【図１５】図１４のＤＶＤレコーダの処理を説明するためのフローチャートである。

【図１６】本発明を適用したＤＶＤレコーダの第４実施の形態の構成例を示すブロック図である。

【図１７】図１６のＤＶＤレコーダの処理を説明するためのフローチャートである。

22

【図１８】本発明を適用したＤＶＤシステムの一実施の形態の構成例を示すブロック図である。

【図１９】図１８のＤＶＤプレーヤ６２の処理を説明するためのフローチャートである。

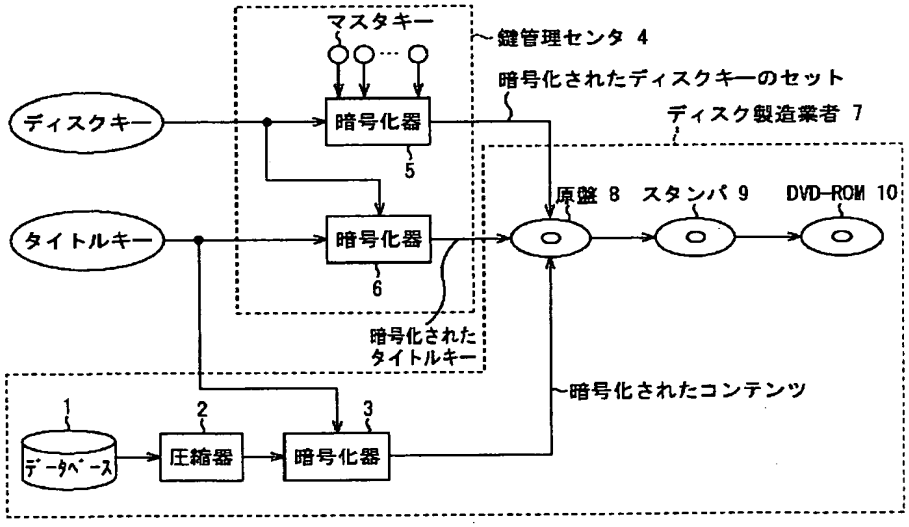
【図２０】本発明を適用したプログラム記録媒体を説明するための図である。

【図２１】図２０のコンピュータ１０１の構成例を示すブロック図である。

【符号の説明】

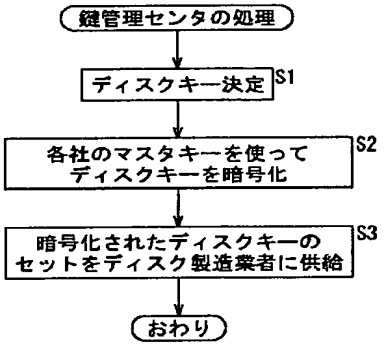
３１　鍵管理センタ，　３２　暗号化器，　３３　ディスク製造業者，　３４原盤，　３５　スタンパ，　３６　ＤＶＤ－ＲＡＭ，　４１　マスタキー記憶部，　４２　復号器，　４３　暗号化器，　４４　タイトルキー生成部，　４５暗号化器，　５１　マスタキー記憶部，　５２乃至５４　復号器，　６１　ＤＶＤレコーダ，　６２　ＤＶＤプレーヤ，　１０１　コンピュータ，　１０２ハードディスク，　１０３　半導体メモリ，　１１１　フロッピーディスク，１１２　CD-ROM，　１１３　MOディスク，　１１４　DVD，　１１５　磁気ディスク，　１１６　半導体メモリ，　１２１　ダウンロードサイト，　１２２　衛星，　１３１　ネットワーク，　１４１　バス，　１４２　CPU，　１４３　ROM，　１４４　RAM，　１４５　入出力インタフェース，　１４６　表示部，　１４７　入力部，　１４８　通信部，　１４９　ドライブ

【図１】

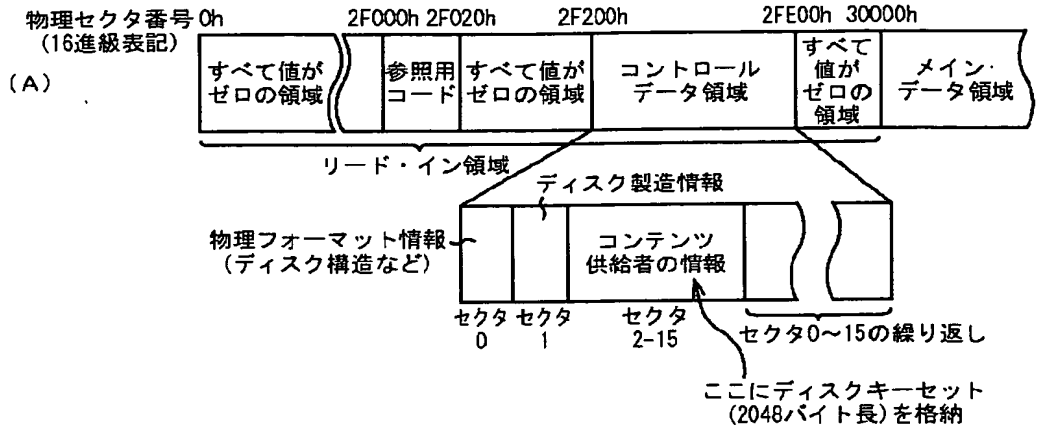


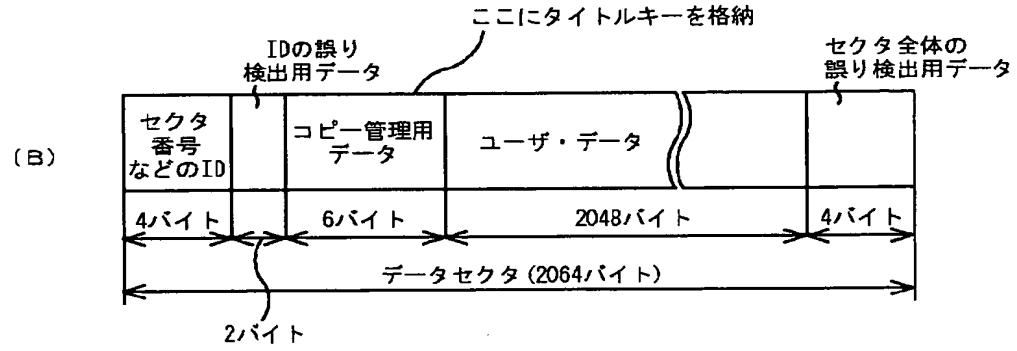
DVD-ROMの製造工程

【図５】

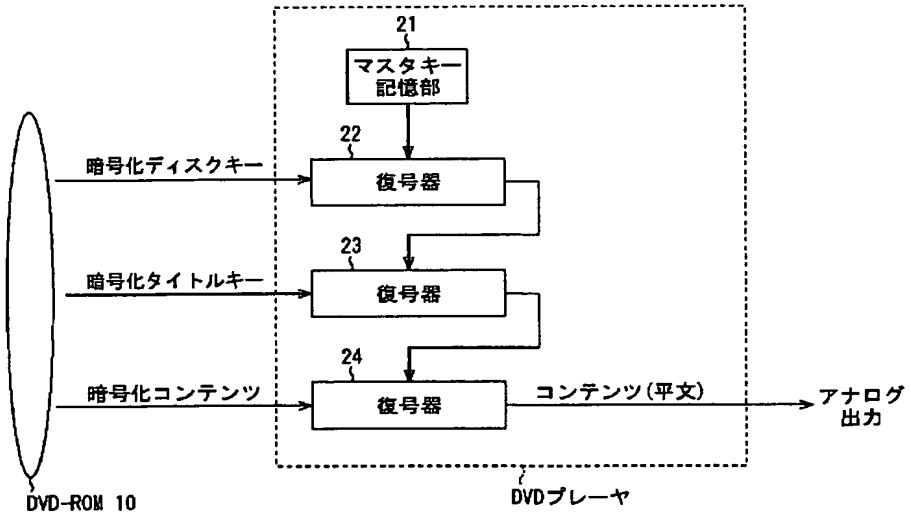


【図２】

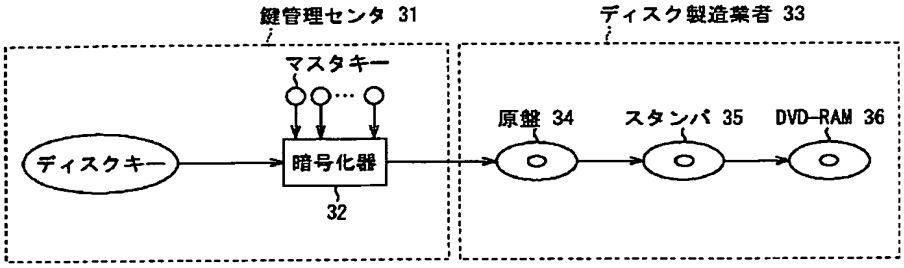

物理セクタ番号 0h
(16進級表記)
2F000h 2F020h
2F200h
2FE00h 30000h
(A)
すべて値が
ゼロの領域
参照用
コード
すべて値が
ゼロの領域
コントロール
データ領域
すべて
値が
ゼロの
領域
メイン
データ領域
リード・イン領域
ディスク製造情報
物理フォーマット情報
(ディスク構造など)
コンテンツ
供給者の情報
セクタ
0
セクタ
1
セクタ
2-15
セクタ0～15の繰り返し
ここにディスクキーセット
(2048バイト長)を格納


(B)
ここにタイトルキーを格納
IDの誤り
検出用データ
セクタ全体の
誤り検出用データ
セクタ
番号
などのID
コピー管理用
データ
ユーザ・データ
4バイト
6バイト
2048バイト
4バイト
データセクタ(2064バイト)
2バイト

【図３】

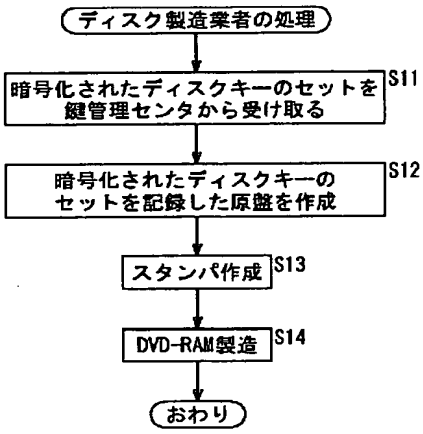

21
マスタキー
記憶部
22
暗号化ディスクキー
復号器
23
暗号化タイトルキー
復号器
24
暗号化コンテンツ
復号器
コンテンツ(平文)
アナログ
出力
DVD-ROM 10
DVDプレーヤ

【図４】

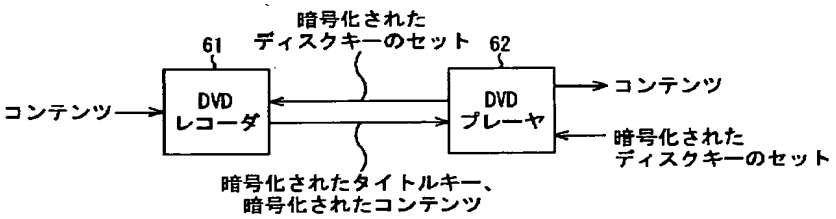


DVD-RAMの製造工程

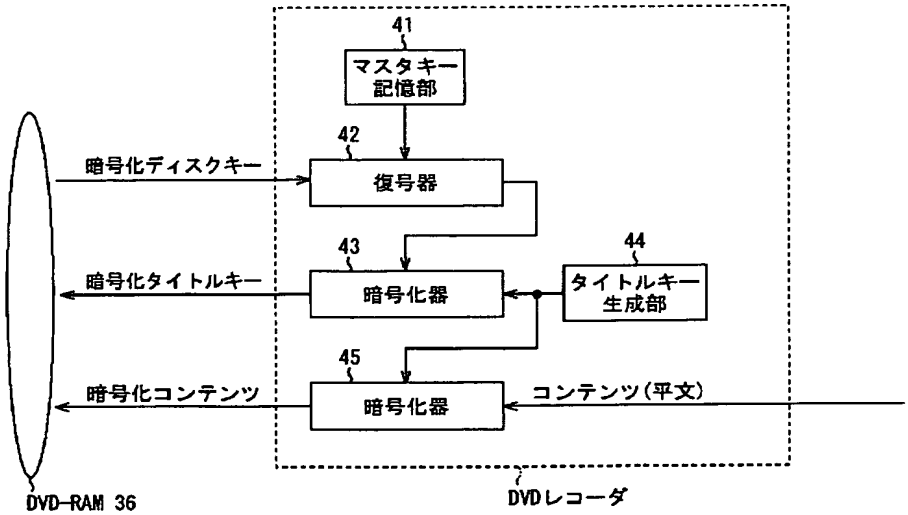
【図６】



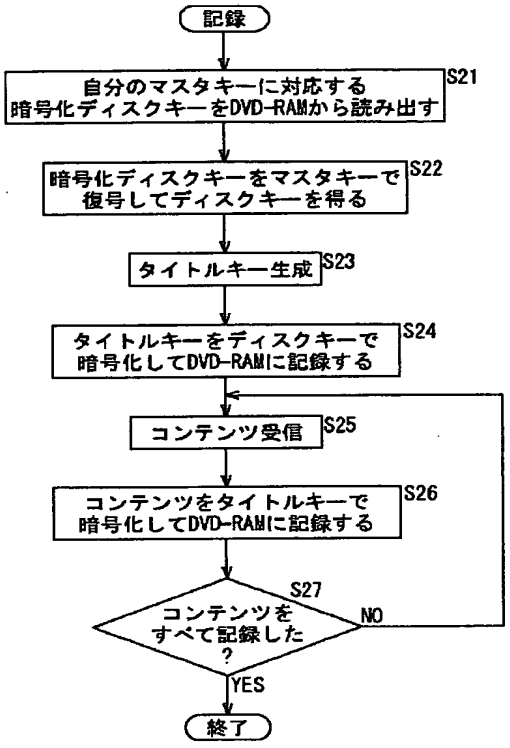
【図１８】



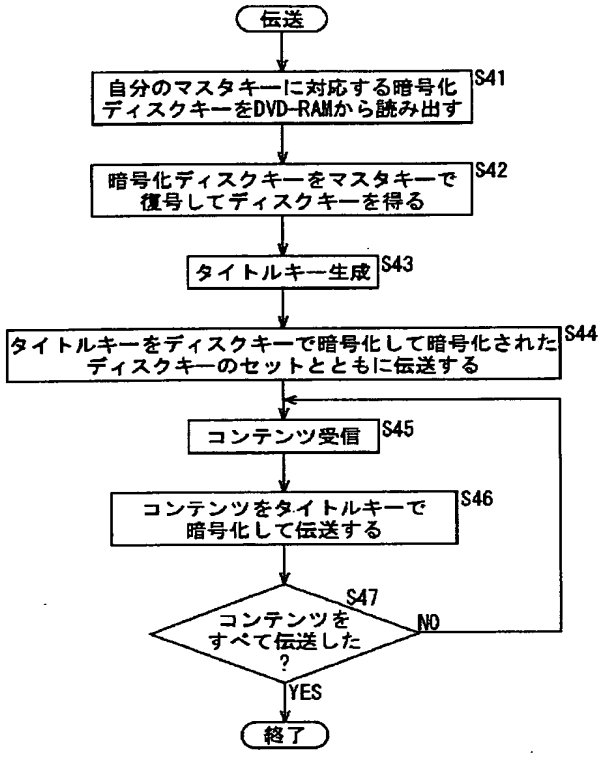
【図７】



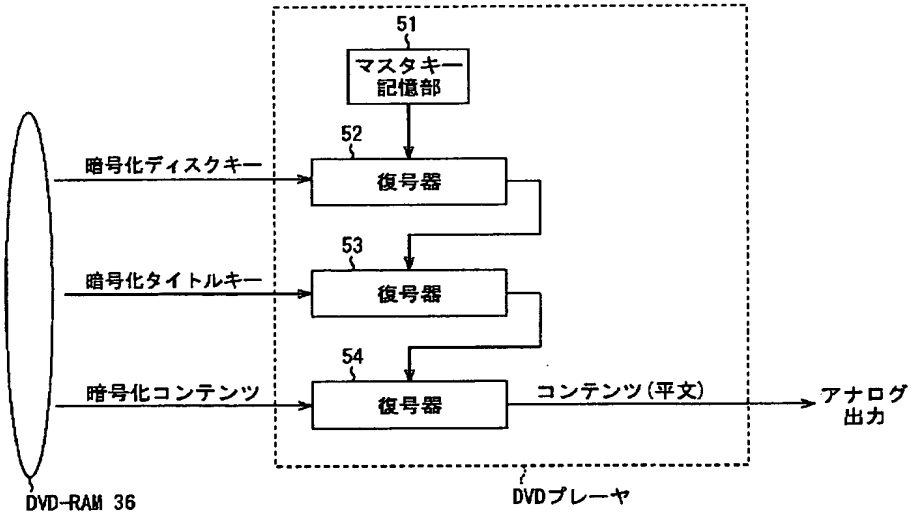
【図８】


記録
自分のマスタキーに対応する暗号化ディスクキーをDVD-RAMから読み出す
S21
暗号化ディスクキーをマスタキーで復号してディスクキーを得る
S22
タイトルキー生成
S23
タイトルキーをディスクキーで暗号化してDVD-RAMに記録する
S24
コンテンツ受信
S25
コンテンツをタイトルキーで暗号化してDVD-RAMに記録する
S26
コンテンツをすべて記録した？
S27
NO
YES
終了

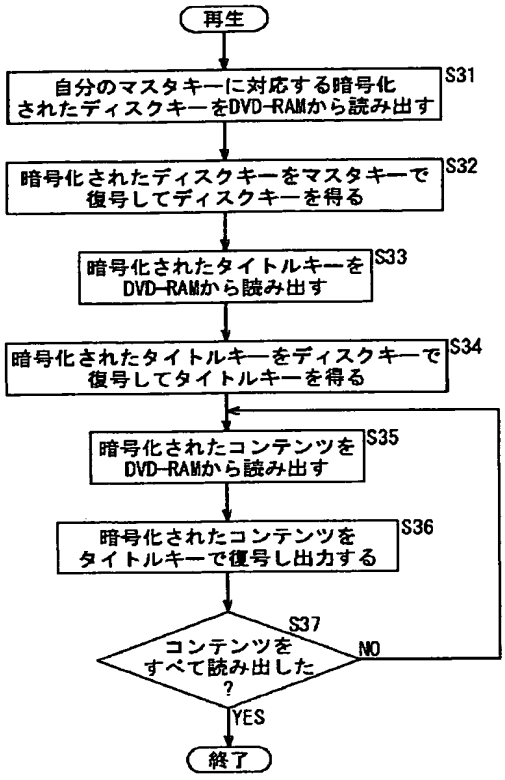
【図１２】


伝送
自分のマスタキーに対応する暗号化ディスクキーをDVD-RAMから読み出す
S41
暗号化ディスクキーをマスタキーで復号してディスクキーを得る
S42
タイトルキー生成
S43
タイトルキーをディスクキーで暗号化して暗号化されたディスクキーのセットとともに伝送する
S44
コンテンツ受信
S45
コンテンツをタイトルキーで暗号化して伝送する
S46
コンテンツをすべて伝送した？
S47
NO
YES
終了

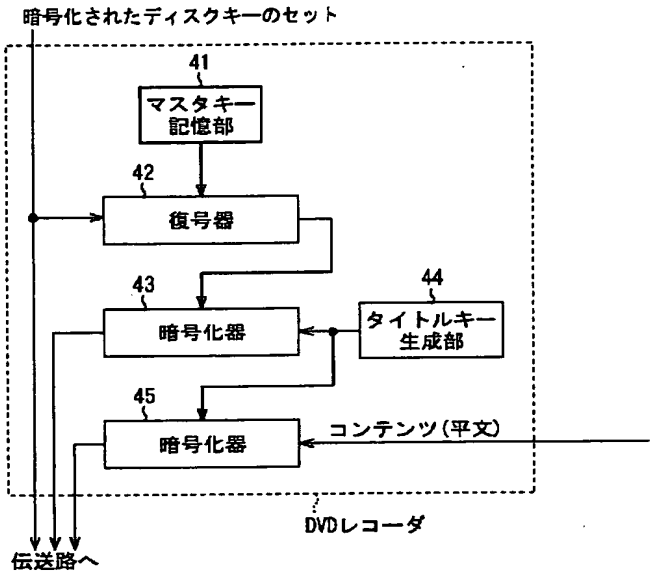
【図９】


51
マスタキー記憶部
52
暗号化ディスクキー
復号器
53
暗号化タイトルキー
復号器
54
暗号化コンテンツ
復号器
コンテンツ(平文)
アナログ出力
DVD-RAM 36
DVDプレーヤ

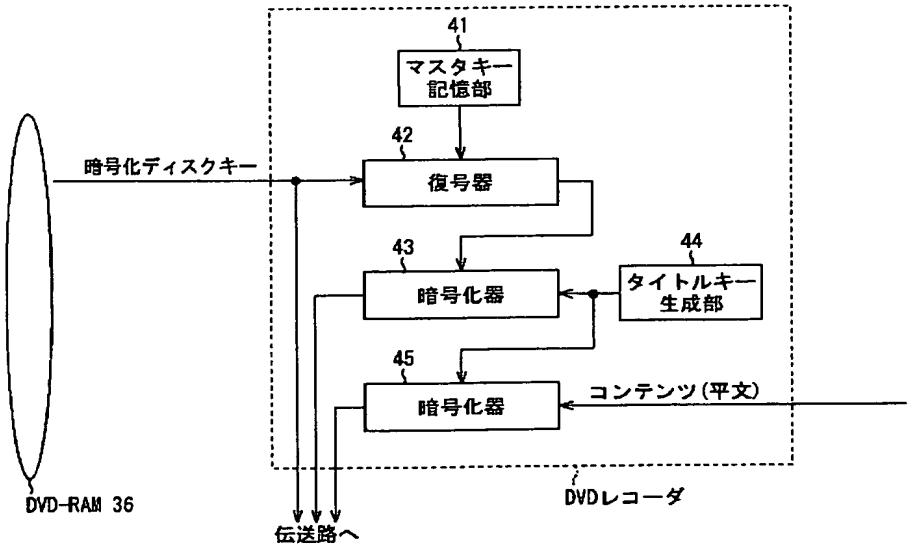
【図１０】


再生
自分のマスタキーに対応する暗号化されたディスクキーをDVD-RAMから読み出す
S31
暗号化されたディスクキーをマスタキーで復号してディスクキーを得る
S32
暗号化されたタイトルキーをDVD-RAMから読み出す
S33
暗号化されたタイトルキーをディスクキーで復号してタイトルキーを得る
S34
暗号化されたコンテンツをDVD-RAMから読み出す
S35
暗号化されたコンテンツをタイトルキーで復号し出力する
S36
コンテンツをすべて読み出した？
S37
NO
YES
終了

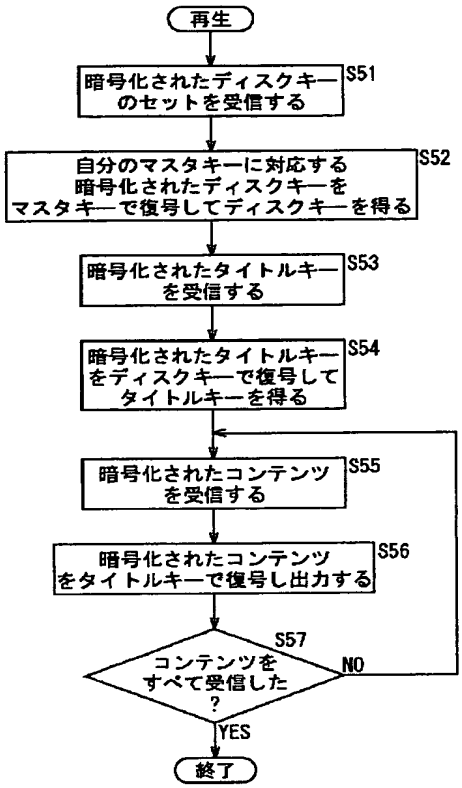
【図１６】


暗号化されたディスクキーのセット
41
マスタキー記憶部
42
復号器
43
暗号化器
44
タイトルキー生成部
45
暗号化器
コンテンツ(平文)
DVDレコーダ
伝送路へ

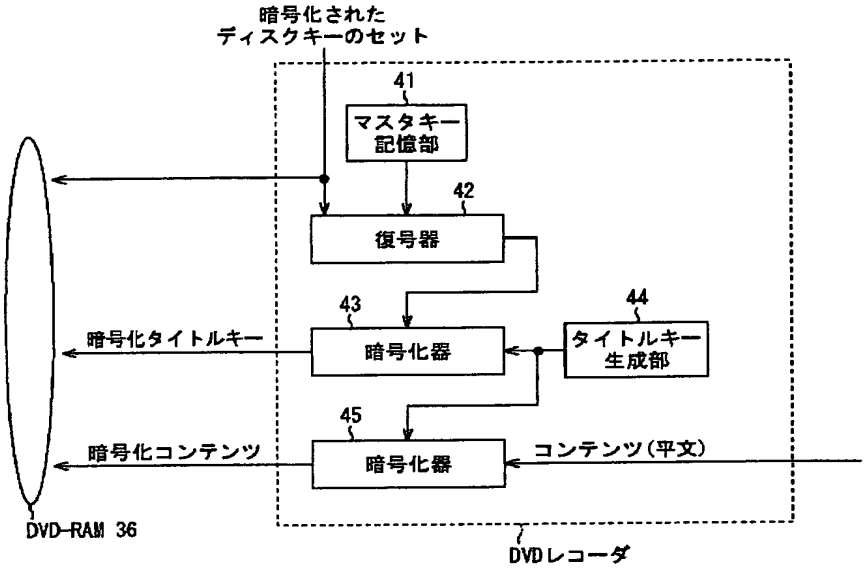
【図１１】


41
マスタキー記憶部
42
暗号化ディスクキー
復号器
43
暗号化器
44
タイトルキー生成部
45
暗号化器
コンテンツ(平文)
DVD-RAM 36
DVDレコーダ
伝送路へ

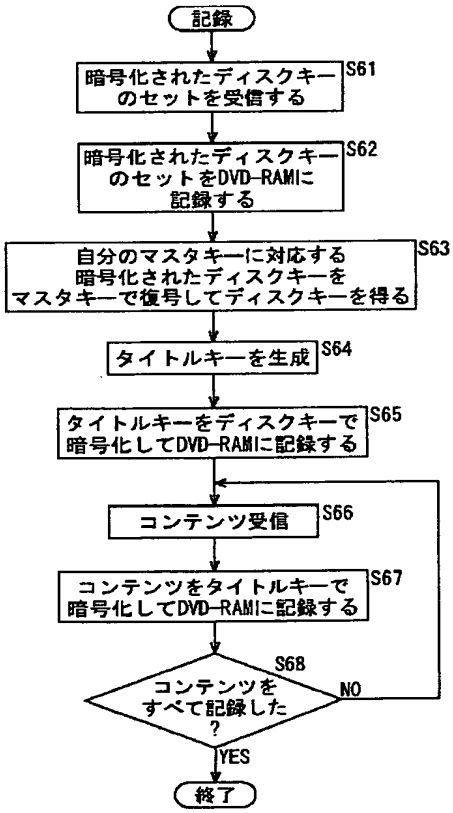
【図１３】


再生
暗号化されたディスクキーのセットを受信する
S51
自分のマスタキーに対応する暗号化されたディスクキーをマスタキーで復号してディスクキーを得る
S52
暗号化されたタイトルキーを受信する
S53
暗号化されたタイトルキーをディスクキーで復号してタイトルキーを得る
S54
暗号化されたコンテンツを受信する
S55
暗号化されたコンテンツをタイトルキーで復号し出力する
S56
コンテンツをすべて受信した？
S57
NO
YES
終了

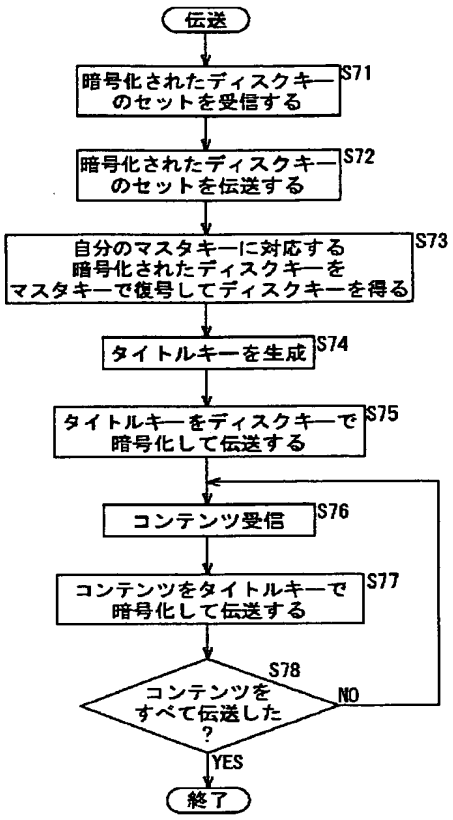
【図１４】


暗号化されたディスクキーのセット
41
マスタキー記憶部
42
復号器
43
暗号化タイトルキー
暗号化器
44
タイトルキー生成部
45
暗号化コンテンツ
暗号化器
コンテンツ(平文)
DVD-RAM 36
DVDレコーダ

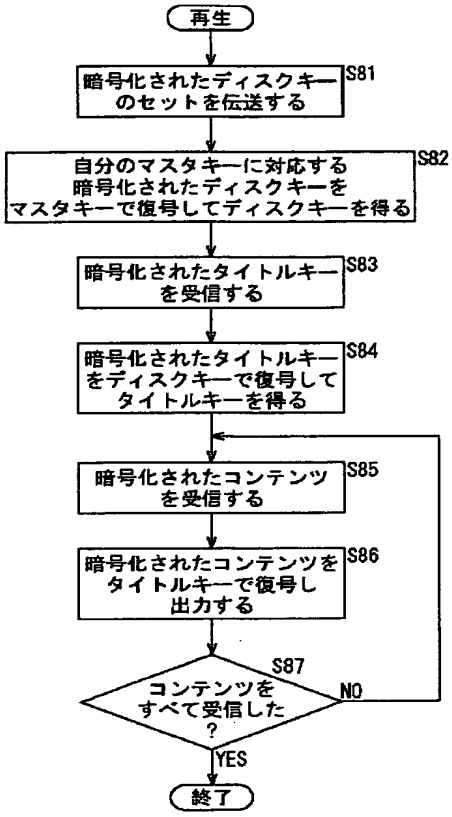
【図１５】


記録
暗号化されたディスクキーのセットを受信する
S61
暗号化されたディスクキーのセットをDVD-RAMに記録する
S62
自分のマスタキーに対応する暗号化されたディスクキーをマスタキーで復号してディスクキーを得る
S63
タイトルキーを生成
S64
タイトルキーをディスクキーで暗号化してDVD-RAMに記録する
S65
コンテンツ受信
S66
コンテンツをタイトルキーで暗号化してDVD-RAMに記録する
S67
コンテンツをすべて記録した？
S68
NO
YES
終了

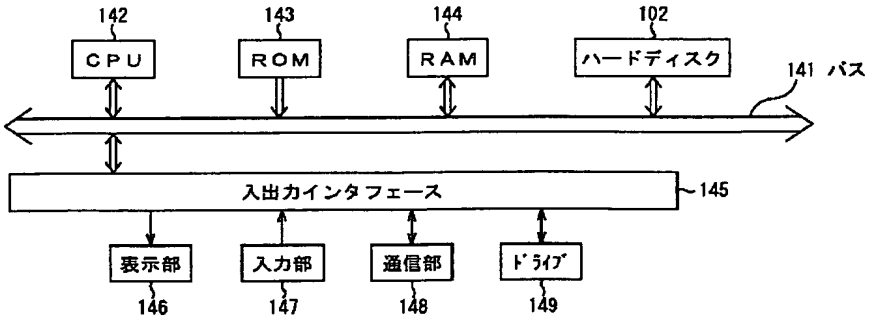
【図１７】



【図１９】

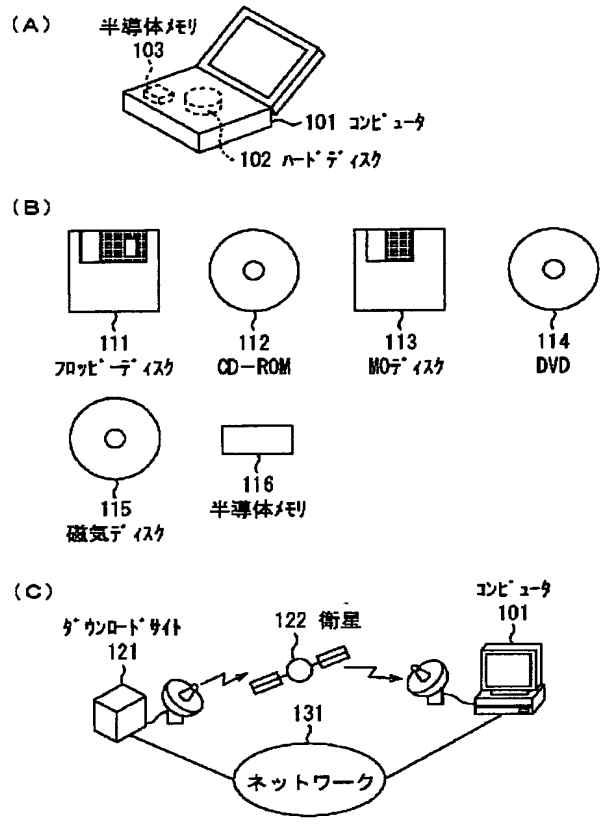


【図２１】



コンピュータ 101

【図２０】



フロントページの続き

(51) Int.Cl.[7]	識別記号	FI		テーマコード(参考)
H04N 5/91		H04L 9/00	601E	
		H04N 5/91	P	

Fターム(参考)　5B017 AA06 BA07 BB02 BB03 CA09
CA16
5C052 AA04 AB03 AB05 CC11 DD04
5C053 FA13 FA25 GA11 GB06 GB21
GB38 JA03
5D044 BC03 CC04 DE49 DE50 EF05
FG18 GK17 HL08 HL11
5J104 AA01 AA12 AA16 EA04 EA06
EA08 EA18 EA22 JA03 NA02
NA03 NA32 PA00 PA14